IT Security Handbook

Extending an Information System Authorization to Operate Process and Templates

ITS-HBK-0006
Effective Date: 20100111
Expiration Date: 20120111
Responsible Office: OCIO/Deputy CIO for Information Technology Security

Contents

Approval

Jerry L. Davis
Deputy Chief Information Officer for
Information Technology Security

1/11/10
Date

Distribution:

NODIS

Change History

Change Number	Date	Change Description

1. Introduction

1.1. This document outlines the procedure for requesting and approving an extension of an Authorization to Operate (ATO) for a NASA information system. This procedure applies to NASA information systems that meet the requirements of NPR 2810.1, including having an existing, unexpired ATO and which have not had any significant changes to the system or its operating environment since the previous assessment and authorization was completed and the ATO was granted.

1.2. ATO Extension requirements include:

1.2.1. An extension to an ATO may be requested and approved in extraordinary circumstances (e.g. a system is being decommissioned or will undergo significant changes within the extension period). ATO extensions are not intended to be used to increase the length of the standard assessment and authorization cycle.

1.2.2. An extension to an ATO may be requested and approved for a single period of up to 6 months. The length of the extension period will be determined on a case by case basis by the Information System Owner (ISO), the appropriate Center Information Technology Security Manager (ITSM) and the information system's Authorizing Official (AO). No additional extensions will be approved within each assessment and authorization cycle.

1.2.2.1. An exception to this requirement is that a second extension request may be submitted for a maximum of 6 additional months when a system is being decommissioned within this extension period.

1.3. Applicable Documents.

a. NPR 2810.1, Security of Information Technology.

b. NIST SP 800-37, Guide for Security Authorization of Federal Information Systems.

2. Process

2.1. The Information System Security Official (ISSO) or equivalent security official and the ISO completes the template in Appendix C of this Handbook and submits it, along with any supporting documentation (including an updated Risk Assessment Report), to the ITSM for concurrence/non-concurrence. The ITSM sends it to the information system AO for final approval or denial of the ATO extension.

2.2. The ITSM reviews and concurs or non-concurs with the proposed ATO extension.

2.3. The AO reviews and makes a determination as follows:

a. **Approved** - The system ATO will be extended for requested time (not to exceed 6 months). (Note: The AO may approve the ATO extension for a lesser period than requested by the ISO but not to exceed the maximum of 6 months.)

b. **Denied** - The system ATO expires on its original expiration date. To continue operating past this date, the system must have successfully completed the assessment and authorization process, as specified in NASA policy and NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

2.4. The ISSO or ISO enters the extension request, including the ITSM recommendation and the AO approval or denial, into the System Security Plan (SSP).

2.5. The ISSO or ISO provides a copy of the approval or denial to the ITSM.

Appendix A. Definitions

Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. [NIST]
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [FIPS 200 adapted]
Information System (Also referred to as IT System)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[44 U.S.C., Sec. 3502] (Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) [NIST]
Information System Security Official	Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. [CNSS Inst. 4009, Adapted]
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST; CNSS 4009, Adapted)
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. [40 U.S.C., Sec. 1401]
Information Technology Security Manager	NASA Center Senior Information Security Officer responsible for assisting the Center CIO in implementing this directive, NASA information security policies and procedures, and the Federal information security laws,

	directives, policies, standards, and guidelines and compliance with the FISMA section 3541 et seq..
Information Technology (IT) System	See information system.
NASA Information	Any knowledge that that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for, or is under the control of NASA. [NPD 2810.1D]
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. [NIST] See *System Security Plan* or *Security Program Plan.*
Significant Change	A modification, deletion, or addition to a system which may result in reducing the effectiveness of protective controls or in making additional protective controls necessary. Examples of significant changes include, but are not limited to, relocation to other facilities, major modification of the existing facilities, introduction of new equipment, addition or deletion of external interfaces, changes to system network connectivity, installation of new operating system software, patches to applications, new releases of software, installation of new application software, introduction of more sensitive data, or a substantial change to the system's risk posture that might affect others on the same network.
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]

Appendix B. Acronyms

AO	Authorization Official
ATO	Authorization To Operate
HBK	Handbook
ISO	Information System Owner
ISSO	Information System Security Official
IT	Information Technology
ITS	Information Technology Security
NIST	National Institute of Standards and Technology
SP	Special Publication
SSP	System Security Plan

Appendix C. Template to Request and Approve an Extension of an ATO for a NASA Information System

Extension Request for NASA Information System Authorization To Operate

System (name, plan number):	Security Impact Level: □ High □ Moderate □ Low
Organization/Center(s):	Date Current ATO Expires:
Length of Requested Extension: □ months	
Reason for Extension:	
Comments/Supporting Documentation (Updated System Security Plan, Risk Assessment Report, schedules, POA&M, etc):	

There have been no significant changes to the above system or its operating environment since the previous assessment and authorization was completed and the ATO was granted.	
System ISSO (name, title, org.):	Contact Information Phone: E-Mail:
ISSO Signature:	Date:
Information System Owner (name, title, org.):	Contact Information Phone: E-Mail:
Information System Owner Signature:	Date:

Center ITSM:

□ Concur

□ Non-Concur
Reason for Non-Concur:

Center ITSM (name, title, org.):	Contact Information Phone: E-Mail:
Center ITSM Signature:	Date:
Authorizing Official (AO): □ Approved □ Denied	
AO (name, title, org.):	
AO Signature:	